

Ref.(4)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-315997

(P2000-315997A)

(43)公開日 平成12年11月14日 (2000.11.14)

(51)Int.Cl.⁷
H 0 4 L 9/08
12/56

識別記号

F I
H 0 4 L 9/00
11/20

テ-マ-ト*(参考)
6 0 1 A 5 J 1 0 4
6 0 1 E 5 K 0 3 0
1 0 2 Z 9 A 0 0 1

審査請求 未請求 請求項の数18 OL (全 22 頁)

(21)出願番号

特願平11-123937

(22)出願日

平成11年4月30日 (1999.4.30)

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 大場 義洋

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72)発明者 野上 和男

東京都日野市旭が丘3丁目1番地の1 株式会社東芝日野工場内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

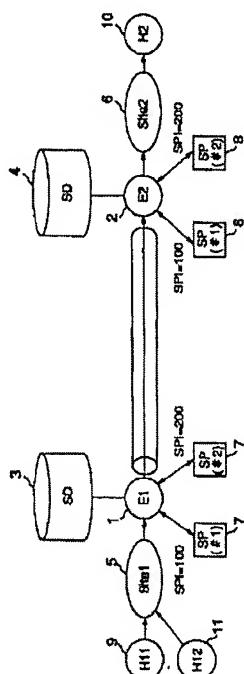
最終頁に続く

(54)【発明の名称】 暗号通信方法及びノード装置

(57)【要約】

【課題】 復号化ノード側におけるパケットの順序保証を考慮した暗号処理の並列化を可能とする暗号通信方法を提供すること。

【解決手段】 暗号側ノード1は、同一の暗号化アルゴリズム・鍵情報を適用して暗号処理を行うべきパケットに、そのパケットヘッダの特定の1個以上のフィールドをハッシュキーとして得たハッシュ値毎に異なる識別子(SPI)を付与する。順序保証を必要とするパケットには同一の識別子が割り当てられる。暗号側ノード1は、該識別子に基づいて並列実行可能な複数の暗号処理装置7の一つを選択し、パケットを暗号化して復号側ノード2に向けて送信する。復号側ノード2は、暗号側ノード1から受信したパケットに付与された識別子(SPI)に基づいて並列実行可能な複数の暗号処理装置8の一つを選択し、該識別子により示される暗号化アルゴリズム・鍵情報を用いて該パケットを復号化する。



【特許請求の範囲】

【請求項1】送信側ノード装置と並列実行可能な複数の暗号処理装置を備えた受信側ノード装置との間でパケットを暗号処理して通信する暗号通信方法において、前記送信側ノード装置は、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケットに、そのパケットが属するグループ毎に異なる識別子を付与し、前記暗号化アルゴリズムおよび鍵情報を適用して第1の暗号処理を施した、前記識別子のパケットを前記受信側ノード装置に向けて送信し、前記受信側ノード装置は、前記送信側ノード装置から受信したパケットに付与された前記識別子に基づいて、前記複数の暗号処理装置のうちの一つを選択し、前記識別子により示される暗号化アルゴリズムおよび鍵情報を適用した、該パケットに対する前記第1の暗号処理に対応する第2の暗号処理を、選択された前記暗号処理装置を用いて行うことを特徴とする暗号通信方法。

【請求項2】前記送信側ノード装置は、前記パケットの識別子に基づいて、並列実行可能な複数の暗号処理装置のうちから、該パケットを処理させるものを選択することを特徴とする請求項1に記載の暗号通信方法。

【請求項3】前記送信側ノード装置は、順序保証を必要とする同一のパケットストリームに所属するパケットには同一の識別子を割り当てる特徴とする請求項1または2に記載の暗号通信方法。

【請求項4】前記送信側ノード装置は、前記パケットのパケットヘッダに含まれる特定の1個以上のフィールドをハッシュキーとして得たハッシュ値に対応して前記異なる識別子を割り当てる特徴とする請求項1に記載の暗号通信方法。

【請求項5】同一の暗号化アルゴリズムおよび鍵情報が適用されるパケットストリームを規定するパケットヘッダの特定の1個以上のフィールドと、前記ハッシュキーとして使用されるパケットヘッダの特定の1個以上のフィールドとを異ならせる特徴とする請求項4に記載の暗号通信方法。

【請求項6】前記識別子を記入する前記パケットの暗号化されないヘッダ内のフィールドを、適用すべき暗号化アルゴリズムおよび鍵情報を特定可能な情報を記述する第1のフィールドおよび前記ハッシュ値を記述する第2のフィールドの少なくとも2つのフィールドに分割することを特徴とする請求項4または5に記載の暗号通信方法。

【請求項7】前記送信側ノード装置と前記受信側ノード装置との間で、前記識別子と適用すべき暗号化アルゴリズムおよび鍵情報との対応に関する設定をプロトコルで自動的に行う場合に、前記第1のフィールドと前記第2のフィールドとのフィールド境界の情報をも該プロトコ

ルで交換することを特徴とする請求項6に記載の暗号通信方法。

【請求項8】前記ハッシュ値を示す情報を、前記パケットの暗号化されないヘッダ内の、前記暗号化アルゴリズムおよび鍵情報を示す情報を記入するフィールド以外の部分に記入することを特徴とする請求項4または5に記載の暗号通信方法。

【請求項9】前記送信側ノード装置と前記受信側ノード装置との間で、前記識別子と適用すべき暗号化アルゴリズムおよび鍵情報との対応に関する設定をプロトコルで自動的に行う場合に、並列処理が可能な暗号処理装置の台数に関するネゴシエーションをも行い、前記送信側ノード装置および前記受信側ノード装置の両方の暗号処理装置の台数の情報を用いて、取り得るハッシュ値の範囲を決定することを特徴とする請求項4ないし8のいずれか1項に記載の暗号通信方法。

【請求項10】暗号処理とレイヤ3のパケットフォワーディングテーブル検索処理とペアにして並列処理することを特徴とする請求項1ないし9のいずれか1項に記載の暗号通信方法。

【請求項11】前記送信側ノード装置における暗号処理は暗号化およびまたは認証情報付与であり、前記受信側ノード装置における暗号処理は復号化およびまたは認証であることを特徴とする請求項1ないし10に記載の暗号通信方法。

【請求項12】パケットを暗号処理して送信するノード装置において、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケットに、当該複数のパケットのうちの一部のパケットとその他の一部のパケットとで異なる識別子を割り当てる割当手段と、前記暗号化アルゴリズムおよび鍵情報を適用して暗号処理を施したパケットに、前記識別子を暗号化せずに付加する手段とを備えたことを特徴とするノード装置。

【請求項13】前記割当手段は、順序保証を必要とする同一のパケットストリームに所属するパケットには同一の識別子を割り当てる特徴とする請求項12に記載のノード装置。

【請求項14】前記割当手段は、前記パケットのパケットヘッダに含まれる特定の1個以上のフィールドをハッシュキーとして得たハッシュ値に対応して前記異なる識別子を割り当てる特徴とする請求項12または13に記載のノード装置。

【請求項15】第1の暗号処理を施されたパケットを受信し、該パケットに対して該第1の暗号処理に対応する第2の暗号処理を施すノード装置において、パケットに付与されている識別子と、該パケットに適用する暗号化アルゴリズムおよび鍵情報を対応付けて記憶する記憶手段と、

50 パケットに対して前記第2の暗号処理を施すための、並

列実行可能な複数の暗号処理手段と、
受信した前記第1の暗号処理を施されたパケットに含まれる前記識別子に基づいて、前記複数の暗号処理手段のうちから、該パケットを処理すべきものを選択する手段と、
前記識別子をもとに前記記憶手段を参照して、選択された前記暗号処理手段が前記パケットに適用すべき暗号化アルゴリズムおよび鍵情報を特定する手段とを備えたことを特徴とするノード装置。

【請求項16】他のノード装置との間で、自装置が送信側または受信側となって、暗号処理されたパケットを通信するノード装置において、

自装置が送信側となる場合に、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケット群のそれぞれのパケットに、その群毎に異なる識別子を付与する手段と、

自装置が受信側となる場合に、受信したパケットに付与された前記識別子に基づいて並列実行可能な複数の暗号処理装置のうちの一つを選択し、該識別子により示される暗号化アルゴリズムおよび鍵情報を用いた該パケットに対する暗号処理を該選択された前記暗号処理装置により行う手段とを備えたことを特徴とするノード装置。

【請求項17】パケットに第1の暗号処理を施して送信し、受信した第1の暗号処理を施されたパケットに対して該第1の暗号処理に対応する第2の暗号処理を施すノード装置において、

自装置が前記第1の暗号処理を施して送信すべきパケットであって、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケット群のそれぞれのパケットに、その群毎に異なる識別子を付与する手段と、

パケットに付与される識別子と、該パケットに適用する暗号化アルゴリズムおよび鍵情報を対応付けて記憶する記憶手段と、

暗号処理して送信すべきパケットに対して前記第1の暗号処理を施すための、並列実行可能な複数の第1の暗号処理手段と、

受信した前記第1の暗号化を施されたパケットに対して前記第2の暗号処理を施すための、並列実行可能な複数の第2の暗号処理手段と、

前記第1の暗号処理を施して送信すべきパケットの前記識別子に基づいて、前記複数の第1の暗号処理装置のうちから、該パケットを処理させるものを選択する手段と、

受信した前記第1の暗号処理を施されたパケットに含まれる前記識別子に基づいて、前記複数の第2の暗号処理手段のうちから、該パケットを処理すべきものを選択する手段と、

受信した前記第1の暗号処理を施されたパケットに含まれる前記識別子をもとに前記記憶手段を参照して、該パ

ケットに適用する暗号化アルゴリズムおよび鍵情報を特定する手段とを備えたことを特徴とするノード装置。

【請求項18】前記第1および第2の暗号処理手段の少なくとも一方は、ネットワークレイヤのパケットフォワーディングテーブルの検索処理を行う手段を含むことを特徴とする請求項17に記載のノード装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、パケットを暗号処理して通信する暗号通信方法及び暗号通信を行うノード装置に関する。

【0002】

【従来の技術】パケットをFIFO(First-In
First-Out)オーダで処理し且つパケットが入力されてから出力されるまでの系内時間が一定でないようなパケット処理系を複数配置して、それらの間で並列処理を行うシステム(可変処理時間並列処理システム)を考える。

【0003】

20 20 このような可変処理時間並列処理システムでは、複数のパケットを並列に処理する結果、系に入る前と後とでパケットの順序逆転が生じる可能性がある。したがって、並列処理の場合には、パケットの順序逆転を防ぐために、(1)システムの出口において、複数のパケット処理系の間でパケット順序の並べ替えを行う方法、または、(2)順序保存が必要なパケットは同一のパケット処理系で処理する方法、のいずれかの方法がとられる。

【0004】上記(1)の方法は、高度に並列化できる反面、並列処理システムの出口でパケットのキューイングやソーティングといった複雑な処理が必要となるため、通常は(2)の方法が使用される。

【0005】上記(2)の方法による並列化を行うシステムの一例として、文献「インターネットドラフト“draft-ietf-fospf-omp-02.txt”」に開示されたものがある。この文献には、あるノードからある宛先ネットワークプレフィックスに対する経路が複数存在し、これらの経路のいずれも使用可能な「マルチパスフォワーディング」の方法が述べられている。同文献では、概略的には、複数の経路のそれぞれを上記可変処理時間並列処理システムにおける1つのパケット処理系とみなし、パケットヘッダ中の送信元アドレスと宛先アドレスとの組からハッシュ値を計算し、ハッシュ値が同じパケットは同じ経路で転送することにより(すなわち同じパケット処理系で処理することにより)、パケットの順序保証を考慮した並列処理を実現している。

【0006】以下、上記のようなパケット処理の並列化を、パケットの暗号処理(暗号化や復号化)に適用した場合の問題点について説明する。

【0007】図20において、101, 111は暗号化

側ノード（アドレスE1、E3）、102は復号化側ノード（アドレスE2）、109、110、119はホスト（H1、H2、H3）、105、106、115はノードE1、2、3側のネットワーク（の集合）、107、108は暗号処理装置である。暗号化側ノードは複数の暗号化装置を持ち、復号化側ノードは複数の復号化装置を持つ。なお、一般に、暗号化装置と復号化装置は両者が組になって1つの暗号処理装置を構成する。

【0008】ここで、1つの暗号処理装置を1つのパケット処理系とみなすと、このパケット処理系におけるパケット処理時間は、パケット長が大きいほど暗号処理（暗号化や復号化）に長時間を要する。このため、複数の暗号処理装置を用いてパケットの暗号処理の並列化を行うシステムは、1つの可変処理時間並列処理システムを形成するとみなすことができる。

【0009】そこで、図20のシステムを見てみると、暗号化側ノードにおける複数の暗号処理装置（SP）を並列化した場合、これが1つの可変処理時間並列処理システムに該当し、同様に、復号化側ノードにおける複数の暗号処理装置（SP）を並列化した場合、これが1つの可変処理時間並列処理システムに該当する。

【0010】この場合、暗号化側ノードでは、上記マルチパスフォワーディングの場合と同様に、パケットのヘッダ情報から計算されたハッシュ値をもとに、パケットの順序保証を考慮した並列化が期待できる。

【0011】ところが、文献「インターネットRFC2401」で定義されるIPsecのトンネルモードのように、（暗号化前の）パケットのヘッダも暗号化するような場合には、復号化側においては、パケットのヘッダ情報は暗号化されており参照できないため、ハッシュ値を計算できず、パケットの順序保証を考慮した復号化処理の並列化を行うことができないという問題点があつた。

【0012】

【発明が解決しようとする課題】上記のように、暗号通信において、1つの暗号処理装置を1つのパケット処理系とみなした可変処理時間並列処理システムを考えた場合、IPsecのトンネルモードのように（暗号化前の）パケットのヘッダも暗号化するような方式では、復号化側において、パケットのヘッダ情報を参照できないため、パケットの順序保証を考慮した復号化処理／認証処理の並列化を行うことができないという問題点があつた。

【0013】本発明は、上記事情を考慮してなされたもので、復号化ノード側におけるパケットの順序保証を考慮した暗号処理の並列化を可能とする暗号通信方法及びノード装置を提供することを目的とする。

【0014】

【課題を解決するための手段】本発明（請求項1）は、送信側ノード装置と並列実行可能な複数の暗号処理装置

を備えた受信側ノード装置との間でパケットを暗号処理して通信する暗号通信方法において、前記送信側ノード装置は、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケットに、そのパケットが属するグループ毎に異なる識別子を付与し、前記暗号化アルゴリズムおよび鍵情報を適用して第1の暗号処理を施した、前記識別子のパケットを前記受信側ノード装置に向けて送信し、前記受信側ノード装置は、前記送信側ノード装置から受信したパケットに付与された前記識別子に基づいて、前記複数の暗号処理装置のうちの一つを選択し、前記識別子により示される暗号化アルゴリズムおよび鍵情報を適用した、該パケットに対する前記第1の暗号処理に対応する第2の暗号処理を、選択された前記暗号処理装置を用いて行うことを特徴とする。

【0015】第1の暗号処理は、例えば、暗号化およびまたは認証情報付与であり、第2の暗号処理は、例えば、復号化およびまたは認証である。識別子は、例えば、セキュリティパラメータインデックス（SPI）である。暗号処理装置は、送信側においては、例えば、暗号化およびまたは認証情報付与の機能を有し、受信側においては、例えば、復号化およびまたは認証の機能を有する。識別子が同一のパケットは、同一の暗号処理装置で処理される。また、識別子が異なるパケットは並列処理ができる。

【0016】好ましくは、前記暗号側ノード装置は、前記パケットの識別子に基づいて、並列実行可能な複数の暗号処理装置のうちから、該パケットを処理させるものを選択するようにしてもよい。

【0017】好ましくは、前記暗号側ノード装置は、順序保証を必要とする同一のパケットストリームに所属するパケットには同一の識別子を割り当てるするようにしてもよい。

【0018】好ましくは、前記暗号側ノード装置は、前記パケットのパケットヘッダに含まれる特定の1個以上のフィールドをハッシュキーとして得たハッシュ値に対応して前記異なる識別子を割り当てるようにしてもよい。

【0019】好ましくは、前記ハッシュキーとして選択可能なフィールドは、送信元アドレス、宛先アドレス、プロトコル番号、送信元ポート番号、宛先ポート番号の任意の組み合わせであるようにしてもよい。

【0020】好ましくは、同一の暗号化アルゴリズムおよび鍵情報が適用されるパケットストリームを規定するパケットヘッダの特定の1個以上のフィールドと、前記ハッシュキーとして使用されるパケットヘッダの特定の1個以上のフィールドとを異ならせるようにしてもよい。

【0021】好ましくは、前記送信側ノード装置と前記受信側ノード装置との間で、前記識別子と適用すべき暗号化アルゴリズムおよび鍵情報との間の関係に関する設

定をプロトコルで自動的に行っててもよい。

【0022】好ましくは、前記識別子を記入する前記パケットの暗号化されないヘッダ内のフィールド（例えば、S P I フィールド）を、適用すべき暗号化アルゴリズムおよび鍵情報を特定可能な情報を記述する第1のフィールドおよび前記ハッシュ値を記述する第2のフィールドの少なくとも2つのフィールドに分割するようにしてもよい。あるいは、好ましくは、前記ハッシュ値を示す情報を、前記パケットの暗号化されないヘッダ内の、前記暗号化アルゴリズムおよび鍵情報を示す情報を記入するフィールド（例えば、S P I フィールド）以外の部分（例えば、T O S フィールド、P r i o r i t y C l a s s フィールド、フローラベルフィールド、L a b e l S t a c k E n t r y のE x p フィールド）に記入するようにしてもよい。なお、上記のいずれの場合においても、好ましくは、前記送信側ノード装置と前記受信側ノード装置との間で、前記フィールドに記述する値（前者では前記第1のフィールドに記述する値のみでよい、後者では該第1のフィールドに相当する前記フィールドに記述する値）と適用すべき暗号化アルゴリズムおよび鍵情報との対応に関する設定をプロトコルで自動的に行っててもよい。また、好ましくは、前者の場合において、前記暗号側ノード装置と前記復号側ノード装置との間で、前記識別子と適用すべき暗号化アルゴリズムおよび鍵情報との対応に関する設定をプロトコルで自動的に行う場合に、前記第1のフィールドと前記第2のフィールドとのフィールド境界の情報をも該プロトコルで交換するようにしてもよい。上記のいずれの場合においても、ハッシュ値を示す情報を記述するフィールド（前者では前記第2のフィールド、後者では例えばT O S フィールド等の当該フィールド）に記述する個々の値（すなわち、個々のハッシュ値）についてネゴシエーションすることは不要となる。また、暗号化アルゴリズムや鍵情報等の設定や特定とは独立して、複数の暗号処理装置への処理の割付が可能となる（暗号化時、復号化時に、パケットの順序保証を考慮した暗号処理の並列化が可能となる）。

【0023】好ましくは、前記暗号側ノード装置と前記復号側ノード装置との間で、前記識別子と適用すべき暗号化アルゴリズムおよび鍵情報との対応に関する設定をプロトコルで自動的に行う場合に、並列処理が可能な暗号処理装置の台数に関するネゴシエーションをも行い、前記暗号側ノード装置および前記復号側ノード装置の両方の暗号処理装置の台数の情報を用いて、取り得るハッシュ値の範囲を決定するようにしてもよい。例えば、（例えば、両者の暗号処理装置の数の最小公倍数-1をハッシュ値の範囲とするようにしてもよい。

【0024】好ましくは、並列して配置する複数の暗号処理装置は、並列配置が可能な任意のパケット処理装置と組にしてもよい。

【0025】好ましくは、暗号処理とレイヤ3のパケットフォワーディングテーブル検索処理とをペアにして並列処理するようにしてもよい。あるいは、暗号装置とフォワーディングテーブル検索装置とを1つのパケット処理装置とし、それらを複数配置して1つの並列処理システムを構成してもよい。

【0026】好ましくは、前記暗号側ノード装置における暗号処理は暗号化およびまたは認証情報付与であり、前記復号側ノード装置における暗号処理は復号化およびまたは認証であるようにしてもよい。例えば、I P s e c の場合には、暗号化はE S Pにより可能であり、認証はE S PあるいはA Hにより可能である。

【0027】また、本発明は、例えばI P s e cに適用可能であり、またその他、I P s e cのS A 識別情報に相当する情報をパケットに付加するような任意のレイヤのセキュリティプロトコルに対して適用可能である。

【0028】本発明（請求項12）は、パケットを暗号処理して送信するノード装置において、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケットに、当該複数のパケットのうちの一部のパケットとその他の一部のパケットとで異なる識別子を割り当てる割当手段と、前記暗号化アルゴリズムおよび鍵情報を適用して暗号処理を施したパケットに、前記識別子を暗号化せずに付加する手段とを備えたことを特徴とする。

【0029】好ましくは、前記割当手段は、順序保証を必要とする同一のパケットストリームに所属するパケットには同一の識別子を割り当てるようにしてもよい。

【0030】好ましくは、前記割当手段は、前記パケットのパケットヘッダに含まれる特定の1個以上のフィールドをハッシュキーとして得たハッシュ値に対応して前記異なる識別子を割り当てるようにしてもよい。

【0031】本発明（請求項15）は、第1の暗号処理を施されたパケットを受信し、該パケットに対して該第1の暗号処理に対応する第2の暗号処理を施すノード装置において、パケットに付与されている識別子と、該パケットに適用する暗号化アルゴリズムおよび鍵情報を対応付けて記憶する記憶手段と、パケットに対して前記第2の暗号処理を施すための、並列実行可能な複数の暗号処理手段と、受信した前記第1の暗号処理を施されたパケットに含まれる前記識別子に基づいて、前記複数の暗号処理手段のうちから、該パケットを処理すべきものを選択する手段と、前記識別子をもとに前記記憶手段を参照して、選択された前記暗号処理手段が前記パケットに適用すべき暗号化アルゴリズムおよび鍵情報を特定する手段とを備えたことを特徴とする。

【0032】好ましくは、前記識別子は、順序保証を必要とする同一のパケットストリームに所属するパケットに対しては、同一の値が割り当てられるようにしてもよい。

【0033】好ましくは、前記識別子は、同一の暗号化アルゴリズムおよび鍵情報を適用すべきパケットであっても、該パケットのパケットヘッダの特定の1個以上のフィールドをハッシュキーとして得たハッシュ値が異なるパケットに対しては、異なる値が割り当たられるようにしてもよい。

【0034】本発明（請求項16）は、他のノード装置との間で、自装置が送信側または受信側となって、暗号処理されたパケットを通信するノード装置において、自装置が送信側となる場合に、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケット群のそれぞれのパケットに、その群毎に異なる識別子を付与する手段と、自装置が受信側となる場合に、受信したパケットに付与された前記識別子に基づいて並列実行可能な複数の暗号処理装置のうちの一つを選択し、該識別子により示される暗号化アルゴリズムおよび鍵情報を用いた該パケットに対する暗号処理を該選択された前記暗号処理装置により行う手段とを備えたことを特徴とする。

【0035】本発明（請求項17）は、パケットに第1の暗号処理を施して送信し、受信した第1の暗号処理を施されたパケットに対して該第1の暗号処理に対応する第2の暗号処理を施すノード装置において、自装置が前記第1の暗号処理を施して送信すべきパケットであって、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数のパケット群のそれぞれのパケットに、その群毎に異なる識別子を付与する手段と、パケットに付与される識別子と、該パケットに適用する暗号化アルゴリズムおよび鍵情報を対応付けて記憶する記憶手段と、暗号処理して送信すべきパケットに対して前記第1の暗号処理を施すための、並列実行可能な複数の第1の暗号処理手段と、受信した前記第1の暗号化を施されたパケットに対して前記第2の暗号処理を施すための、並列実行可能な複数の第2の暗号処理手段と、前記第1の暗号処理を施して送信すべきパケットの前記識別子に基づいて、前記複数の第1の暗号処理装置のうちから、該パケットを処理させるものを選択する手段と、受信した前記第1の暗号処理を施されたパケットに含まれる前記識別子に基づいて、前記複数の第2の暗号処理手段のうちから、該パケットを処理すべきものを選択する手段と、受信した前記第1の暗号処理を施されたパケットに含まれる前記識別子をもとに前記記憶手段を参照して、該パケットに適用する暗号化アルゴリズムおよび鍵情報を特定する手段とを備えたことを特徴とする。

【0036】好ましくは、順序保証を必要とする同一のパケットストリームに所属するパケットには同一の識別子を割り当てるようにもよい。

【0037】好ましくは、前記パケットのパケットヘッダの特定の1個以上のフィールドをハッシュキーとして得たハッシュ値に対応して異なる識別子を割り当てるよ

うにしてもよい。

【0038】好ましくは、前記暗号処理装置は、ネットワークレイヤのパケットフォワーディングテーブルの検索処理を行う手段を含むようにしてもよい。

【0039】好ましくは、前記第1および第2の暗号処理手段の少なくとも一方は、ネットワークレイヤのパケットフォワーディングテーブルの検索処理を行う手段を含むようにしてもよい。

【0040】また、本発明のノード装置は、ルータと暗号処理装置とが一体となっていてもよく、またルータと暗号処理装置とが独立していてもよい。ノードと暗号処理装置とが独立の場合には、それらはネットワークを介して接続してもよく、さらに複数のルータで1つ以上の暗号処理装置を共有してもよい。

【0041】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0042】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読み取り可能な記録媒体としても成立する。

【0043】本発明において、送信側ノード装置では、暗号処理するパケットに適用する暗号化アルゴリズムおよび鍵情報を決定する処理を行う。このためには、例えば、ある暗号化アルゴリズムおよび鍵情報が適用されるパケットフローを規定するセレクタを利用することができます。使用可能なセレクタとしては、（a）パケットの宛先アドレスまたは宛先アドレスのリスト、（b）パケットの送信元アドレスまたは送信元アドレスのリスト、（c）プロトコル番号、（d）送信ポート番号と受信ポート番号、などがある。

【0044】送信側ノード装置・受信側ノード装置間を転送される暗号化パケットには、少なくとも前記識別子（例えば、セキュリティパラメータインデックス（S P I））が付加される。この識別子は、暗号化アルゴリズムおよび鍵情報と関連付けられる。また、この識別子は、暗号化せずにパケットに付加されて、送信側から受信側へ伝えられる。

【0045】本発明では、送信側ノード装置は、同一の暗号化アルゴリズムおよび鍵情報を持つパケットであっても、他の基準によって、異なる識別子を割り当てることが可能である。例えば、パケットのパケットヘッダの特定の1個以上のフィールドをハッシュキーとして得たハッシュ値に対応して異なる識別子を割り当てることができる。その際、順序保証を必要とする同一のパケットストリームに所属するパケットには同一の識別子を割り当てる。

【0046】さて、本発明では、受信側ノード装置は、並列実行可能な複数の暗号処理装置を備えており、送信側ノード装置から受信した暗号化等されたパケットを復号化等する場合には、該パケットに付与された識別子に基づいて該複数の暗号処理装置のうちの一つを選択し、該識別子により示される暗号化アルゴリズムおよび鍵情報による該パケットに対する復号化等を、該選択した暗号処理装置を用いて行う。

【0047】また、並列実行可能な複数の暗号処理装置を備えている送信側ノード装置でも、識別子に基づいて該複数の暗号処理装置のうちの一つを選択するようになることができる。

【0048】本発明によれば、パケットに暗号化せずに付加されている上記識別子に基づいて該パケットを処理する暗号処理装置を選択するので、同一の識別子が割り当てられたパケットは同一の暗号処理装置で処理されることになり、同一の識別子を割り当てたパケットについて順序保証することが可能となる。

【0049】例えば、順序保証を必要とする同一のパケットストリームに所属するパケットに同一の識別子を割り当てれば、それらパケットを順序保証することができる。

【0050】また、例えば、順序保証を必要としないパケット間には異なる識別子を割り当てることができる。そして、識別子の異なるパケットは、異なる暗号処理装置に振り分けることができるので、パケットの順序保証を確保した上で、並列処理を行うことができる。

【0051】また、本発明では、同じ暗号化アルゴリズム・鍵情報を適用すべきパケットであっても、順序保証を必要としないパケット間には異なる識別子を割り当てができるようになっているので、処理の並列性をより高めることができる。例えば、ある暗号化アルゴリズム・鍵情報を適用すべきパケットが多量になった場合でも、処理を分散させることができる。また、同じ鍵情報を使用することができるので、鍵が少なくて済む、セレクタが簡単になる、という利点もある。

【0052】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0053】まず、本実施形態の基本的な事項について説明する。

【0054】暗号側ノードおよびまたは復号側ノードとしての機能を有するようなノードを総称して、「暗号処理ノード」と呼ぶものとする。また、暗号側ノードにおける暗号化処理や認証情報付与処理および復号側ノードにおける復号化処理や認証情報に基づく認証処理等を総称して、「暗号処理」と呼ぶものとする。また、1種類または数種類の暗号処理を行う機能を有する装置を総称して、「暗号処理装置」と呼ぶものとする。

【0055】順序保証が必要なパケットとは、例えば、

送信元アドレス、宛先アドレス、送信ポート番号、受信ポート番号、プロトコル番号の全てが同一のパケットストリームに属するパケットである。

【0056】本実施形態では、IPsec（インターネットRFC2401）を具体例に利用して説明する。

【0057】本実施形態では、暗号側ノード（送信側ノード）と復号側ノード（受信側ノード）との間を転送される暗号化パケットには、そのパケットに適用する「セキュリティアソシエーション」を識別するための「セキュリティアソシエーション識別情報（以下、SA識別情報と略記する）」が付加される。

【0058】本実施形態では、「セキュリティアソシエーション（SA：Security Association；以下、SAと略記することもある）」の内容には、セキュリティプロトコル、暗号化アルゴリズム、鍵情報が含まれる。本実施形態では、SA識別情報は、「セキュリティパラメータインデックス（SPI：Security Parameter Index）」、「そのパケットが復号化されるべきノードのアドレス（すなわちIPsecのトンネルモードにおけるトンネル出口のノードのアドレス）」、「セキュリティプロトコル」の3つ情報の組からなる。

【0059】また、本実施形態では、暗号側ノードにおいて、暗号化するパケットに適用するセキュリティアソシエーションを決定する処理を行うが、このために、あるセキュリティアソシエーションが適用されるパケットフローを規定する「セレクタ」を利用する。使用可能なセレクタとしては、(a) パケットの宛先アドレスまたは宛先アドレスのリスト、(b) パケットの送信元アドレスまたは送信元アドレスのリスト、(c) プロトコル番号、(d) 送信ポート番号と受信ポート番号、などがある。例えば、(a)の場合、同じ宛先アドレスを持つパケットを一纏まりとして、それらに同じセキュリティアソシエーションを適用することにする。なお、詳しくは後述するように、SAの内容が同一のパケットには同一のSA識別情報が付されるようにする方法の他に、SAの内容が同一のパケットの間でさらに他の基準によって（例えばハッシュを使って）、パケットを異なるSA識別情報（SPIが異なるもの）に振り分ける方法がある（後者の方法は、例えば、セキュリティアソシエーションが同じパケットを複数の暗号処理装置に分散させることができるようにする目的で使用する）。

【0060】また、SAの内容およびSA識別情報に含まれる5種類の情報の組み合わせ方に対する制約について、例えば、1 SPIのみ異なる組み合わせを使用可能とする方法、使用可能としない方法、2異なる（トンネル出口）ノードアドレスに対して同じSPIを重複して割り当てる方法、可能としない方法、3異なるセキュリティプロトコルに対して同じSPIを重複して割り当てる方法、可能としない方法、などが幾

つかの制約が考えられるが、どのような制約を課すかによつては、SA識別情報の一部（例えばSPI）のみでSAを特定できる場合がある。復号側ノードでは、パケットを復号化する際に、（暗号化されたもとのパケットヘッダ内に書き込まれている情報を使用することなしに）そのパケットに適用するSAを特定する処理を行うが、本実施形態では、暗号化パケットに暗号化されずに付加されているSPIのみでSAを特定する場合の例を中心に説明する。

【0061】また、暗号処理ノード（暗号側ノードおよびまたは復号側ノードとしての機能を有するノード）は、パケットを暗号処理（暗号化・復号化）する暗号処理装置を複数備えており、暗号処理する際に、各パケットを暗号処理させる暗号処理装置を選択する処理を行うが（特に復号側ノードでは暗号化されたもとのパケットヘッダ内に書き込まれている情報を使用することなしに該選択を行う必要がある）、本実施形態では、パケットに暗号化されずに付加されるSPIのみで該パケットを暗号処理させる暗号処理装置を特定する場合の例を中心に説明する。

【0062】本実施形態では、順序保証する必要のあるパケットは、必ず同一の暗号処理装置で暗号処理されるので、確実に順序が保証される。また、暗号処理ノードが有する複数の暗号処理装置の処理の並列性を高めることが可能となる。

【0063】ところで、本実施形態では、同じセキュリティプロトコル、暗号化アルゴリズム、鍵情報を用い、かつ、SA識別情報が異なるようなSAを複数持つような構成も可能である。このとき、SA識別情報が異なるパケットは、異なる暗号処理装置を用いて並列に暗号処理を行うことが可能である。

【0064】また、本実施形態では、（同一のトンネル出口ノードアドレスに対して、）同じセキュリティプロトコル、暗号化アルゴリズム、鍵情報を用い、かつセキュリティパラメータインデックス（SPI）が異なるようなセキュリティアソシエーション（SA）を複数もつのような構成も可能である。このとき、SPIが異なるパケットは、異なる暗号処理装置を用いて並列に暗号処理を行うことが可能である（ただし、SA識別情報すなわちSAが異なっていても、SPIが同じになる場合がある；トンネル出口ノードアドレスかセキュリティプロトコルが異なる）。このとき、（1）パケットのヘッダ情報から、セキュリティプロトコル、暗号化アルゴリズム、鍵情報を決定するとともにハッシュ値を計算し、ハッシュ値が異なるパケットには異なるSPIを割り当てるようにする方法、（2）SPIをSA識別用のフィールドと、ハッシュ値用のフィールドの少なくとも2つのサブフィールドに分割する方法などが考えられる。

【0065】ハッシュ値を計算する際に使用するハッシュキーは、SAのセレクタと異なり、かつ、ハッシュ値

が異なるパケット間で順序保証が必要ないようなものを選ぶのが好ましい。（2）の場合には、2つのサブフィールドの境界は暗号化側と復号化側のノードの設定により変更可能である。また、ISAKMPなどのセキュリティアソシエーションや鍵情報をネゴシエーションするプロトコルを用いて境界の情報を暗号化側と復号化側のノード間で交換してもよい。

【0066】これにより、セキュリティプロトコル、暗号化アルゴリズム、鍵情報を1種類しか使用しない場合にも、暗号化時、復号化時の両方でパケットの順序保証を考慮した暗号処理の並列化が可能となる。

【0067】このような方法は、IPsecのトンネルモードの場合に、あるトンネルに対して单一のセキュリティプロトコル、暗号化アルゴリズム、鍵情報のみ定義する場合、すなわち、1個のセレクタのみ定義する場合に、セレクタの数が多い場合に比べ、セキュリティアソシエーションを決定するのにかかる検索時間を大幅に減らしつつ暗号処理の高速化が期待できる。

【0068】さて、以下では、本暗号通信システムの全体的な構成例を幾つか示し、さらにノードの構成や処理手順について説明する。

【0069】なお、以下では、セキュリティプロトコルが暗号化ペイロードである場合（送信側で暗号化を行い、受信側で復号化を行う場合）を中心に説明するが、セキュリティプロトコルが認証ヘッダの場合（送信側で認証情報付与を行い、受信側で認証を行う場合）、およびセキュリティプロトコルが認証情報つきの暗号化ペイロードである場合（送信側で暗号化および認証情報付与を行い、受信側で認証および復号化を行う場合）も基本的に同様である（基本的には暗号処理の内容が変わるものである）。

【0070】まず、本暗号通信システムの第1の構成例について説明する。

【0071】第1の構成例では、IPsecにおいて、セキュリティアソシエーション（SA）が複数種類存在する場合の暗号処理の並列化の例を示す。

【0072】図1に、本発明を適用する通信ネットワークの一例を示す。

【0073】図1のネットワークにおいて、1は暗号化側ノード（アドレスをE1とする）（以下、ノードE1と記述する）、2は復号化側ノード（アドレスをE2とする）（以下、ノードE2と記述する）、9～11はホスト（アドレスをそれぞれH11、H2、H12とする）、5はノードE1側のネットワーク（の集合）（以下、Site1と記述する）、6はノードE2側のネットワーク（の集合）（以下、Site2と記述する）、7、8は暗号処理装置（SP：Security processor）、3、4はセキュリティデータベース（SD：Security Database）である。

【0074】なお、図1において、他の暗号処理ノードやネットワークやホストが存在してもよい。また、暗号処理ノードは、複数の他の暗号処理ノードに接続されている場合において、接続される暗号処理ノード毎に異なるアドレスを持つてもよい。

【0075】図1において、ノードE1をトンネルの入口とし、ノードE2をトンネルの出口とするIPsecトンネルが存在するものとする。すなわち、ノードE1は、Site2に属するホスト宛のパケットは、必要であればIPsecで暗号化して“宛先アドレス=E2”としてIPパケットにカプセル化して送信する。また、ノードE2は、IPsecトンネルを介してノードE1から転送してきた“宛先アドレス=E2”とする暗号化カプセル化パケットを受信し、必要であれば復号化（およびデカプセル化）を行う。

【0076】セキュリティデータベース（SD）は、IPsecの場合には、論理的に、セキュリティポリシーデータベース（SPD：Security Policy Database）と、セキュリティアソシエーションデータベース（SAD：Security Association Database）との2つに分かれ。SPDは、パケットを暗号化してトンネル上に転送するか、または暗号化せずにトンネル上に転送するか、または廃棄するか、についての情報を含むデータベースである。一方、SADは、パケットを暗号化する場合に用いる暗号化のパラメータ情報（使用する暗号化アルゴリズム、鍵情報、SPIなど）を含むデータベースである。本実施形態では、SPDとSADとを一つのデータベースとして構成した例を用いているが、SPDとSADとを別々のデータベースとして構成しても構わない。

【0077】図2に、ノードE1やノードE2が管理するセキュリティデータベース（SD）の一例を示す。

【0078】図2では、まず、トンネル出口のノードのアドレスとセレクタとセキュリティポリシーとを参照すると、トンネル出口のノードのアドレスがE2であるようなパケットのうち、送信元アドレスがH11またはH12のパケットが暗号化されてトンネル上で転送され、その他のSite2に属するパケットは暗号化されずにトンネル上に転送され、トンネル出口のノードのアドレスがE2以外であるようなパケットは廃棄されることになる。

【0079】また、暗号化して転送するパケットについては、トンネルの出口がノードE2であるようなパケットのうち、送信元アドレスがH11のパケットは、セキュリティプロトコル=ESP（Encapsulation Security Payload）、暗号化アルゴリズム=A1、鍵=K1、SPI=100のセキュリティアソシエーション（SA）にマッピングされることになる。一方、トンネルの出口がノードE2であるようなパケットのうち、送信元アドレスがH12のパケッ

トは、セキュリティプロトコル=ESP、暗号化アルゴリズム=A2、鍵=K2、SPI=200のセキュリティアソシエーション（SA）にマッピングされることになる。

【0080】暗号処理装置7は、少なくとも、暗号側ノードにとって必要な暗号処理機能を有する。暗号処理装置8は、少なくとも、復号側ノードにとって必要な暗号処理機能を有する。なお、ノードE1およびノードE2はいずれも暗号側ノードとしても復号側ノードとしても機能できるようにするのが好ましく、この場合には、暗号処理装置7と暗号処理装置8とは同じものであり、暗号側ノードに必要な暗号処理機能と復号側ノードに必要な暗号処理機能の両方を有する。

【0081】ノードE1は複数の暗号処理装置7を持つており、これらの暗号処理装置同士は並列に暗号化処理を行うことができるものとする。同様に、ノードE2は複数の暗号処理装置8を持っており、これらの暗号処理装置同士は並列に復号化処理を行うことができるものとする。

【0082】本実施形態では、各パケットに対応するSPIに基づいて、該パケットを処理すべき暗号処理装置を複数のうちから選択する。例えば、図3に示すように、ノードE1では、パケットを暗号化する際に、SPI=100のパケットとSPI=200のパケットとを、異なる暗号処理装置に割り振って暗号化させる。同様に、ノードE2では、暗号化されたパケットを復号化する際に、SPI=100のパケットとSPI=200のパケットとを、異なる暗号処理装置に割り振って復号化させる。もちろん、各暗号処理装置は、ノードE1が使用する暗号化アルゴリズムに対応する復号化アルゴリズムおよび鍵を使用する。

【0083】ここで、図2および図3の例においてトンネル出口のノードのアドレスをE2とし、送信元アドレスをH11/H12とするパケットを暗号通信する場合の手順の一例を示す。

【0084】まず、ノードE1では、図2を参照し（セレクタに基づいて）、トンネル出口のノードのアドレスをE2とし、送信元アドレスをH11とする該パケットを、セキュリティプロトコルESP、暗号化アルゴリズムA1、鍵情報K1によって暗号化し、SPI=100として、送信する。

【0085】また、トンネル出口のノードのアドレスをE2とし、送信元アドレスをH12とする該パケットを、セキュリティプロトコルESP、暗号化アルゴリズムA2、鍵情報K2によって暗号化し、SPI=200として、送信する。

【0086】その際、SPI=100であるパケットは、#1の暗号処理装置で処理し、SPI=100であるパケットは、#2の暗号処理装置で処理する。

【0087】ノードE2では、トンネル出口のノードの

アドレスをE2とし、S P I = 100とするパケットを、セキュリティプロトコルESP、暗号化アルゴリズムA1、鍵情報K1によって復号化する。

【0088】また、トンネル出口のノードのアドレスをE2とし、S P I = 200とするパケットを、セキュリティプロトコルESP、暗号化アルゴリズムA2、鍵情報K2によって復号化する。

【0089】その際、S P I = 100であるパケットは、#1の暗号処理装置で処理し、S P I = 100であるパケットは、#2の暗号処理装置で処理する。

【0090】なお、S P Iによって暗号処理装置を決定する場合、S P Iの種類が暗号処理装置の個数よりも多い。この場合、複数種類のS P Iのパケットを同じ番号の暗号処理装置に重複して割り振ればよい。また、割り振り方にも種々の方法が考えられる。

【0091】また、暗号側ノードの持つ暗号処理装置の個数と復号側ノードの持つ暗号処理装置の個数とは、同数でなくても構わない。また、暗号側ノードと復号側ノードとの間の暗号通信において使用する暗号処理装置の個数は、暗号側ノードと復号側ノードとで異なっても構わない。

【0092】また、上記では、セキュリティパラメータインデックス(S P I)のみを参照して、複数の暗号処理装置にパケットを振り分ける場合を示したが、SA識別情報(トンネル出口アドレス、S P I、セキュリティプロトコル)全体を見て複数の暗号処理装置にパケットを振り分けることも可能である。

【0093】また、S P IのみでセキュリティアソシエーションSAを識別できるようにするために、SA識別情報の(トンネル出口アドレス、セキュリティプロトコル)の組が異なるセキュリティアソシエーション間でS P Iの重複を許さないようにした場合には、暗号処理装置においてS P Iのみ参照するだけで、セキュリティアソシエーション(セキュリティプロトコル、暗号化アルゴリズム、鍵情報)を一意に決めることが可能である。

【0094】また、各パケットの複数の暗号処理装置に対する割り振り方法として、暗号側ノードと復号側ノードとでは異なる方法を用いてもかなわない(暗号側ノードでは、S P Iによらない方法を用いることも可能である)。

【0095】次に、本暗号通信システムの第2の構成例について説明する。

【0096】ここでは、I P s e cにおいて、(同一のトンネル出口ノードアドレスに対して、)セキュリティパラメータインデックス(S P I)は互いに異なるが、セキュリティプロトコルと暗号化アルゴリズムと鍵情報は全て同一であるような複数のセキュリティアソシエーションの設定を許容し、それらセキュリティアソシエーション間で暗号化処理の並列化を行う場合について説明する。また、ここでは、パケット内に記述されて転送さ

れるS P Iにハッシュ値を埋め込まない場合の例を示す。

【0097】ネットワーク構成は図1の例と同様である、図4に、この場合のノードE1とノードE2が管理するセキュリティデータベース(S D)の一例を示す。なお、図4では、説明を簡単にするために、「指定なし(全てのパケット)」という内容のセレクタを用いている。

【0098】図4の内容によれば、トンネル出口のノードのアドレスがE2であるようなパケットは、(セレクタを指定なしとしているので)すべて暗号化されてトンネル上で転送される。トンネルの出口のノードのアドレスがE2以外であるようなパケットは廃棄される。

【0099】また、トンネル出口のノードのアドレスがE2であるようなパケットは、後述する基準によって、「セキュリティプロトコル=ESP、暗号化アルゴリズム=A1、鍵=K1、S P I=100のセキュリティアソシエーション(S A)」と、「セキュリティプロトコル=ESP、暗号化アルゴリズム=A1、鍵=K1、S P I=200のセキュリティアソシエーション(S A)」とのいずれかにマッピングされる。

【0100】同一のセレクタに対して複数のセキュリティパラメータインデックス(S P I)が割当て可能な場合には、振り分けの基準としては、次のようなものが考えられる。例えば、まず、セレクタ毎に、Hの各々の値に対して、1つのS P Iを対応させておく。そして、暗号化することになったパケットについて、その暗号化前のI PパケットヘッダおよびまたはI Pペイロードのフィールドの全部または一部の情報を用いて、そのパケットのハッシュ値(H)を計算する。これによって、パケットがマッチしたセレクタと、計算されたHの値から、使用するS P Iが一意に定まる。

【0101】図4においては、「指定なし」のセレクタに対して、ハッシュ値H=0にはS P I=100が対応し、ハッシュ値H=1にはS P I=200が対応する。

【0102】ただし、図4において、ハッシュ値Hのフィールドは復号化側のセキュリティデータベース(S D)には必要ない。

【0103】このとき、図3に示すように、ノードE1では、パケットを暗号化する場合に、S P I=100のパケットとS P I=200のパケットは、異なる暗号処理装置S Pで暗号化を行う。このとき、両方の暗号処理装置は、同じ暗号化アルゴリズムおよび鍵を使用する。

【0104】同様に、ノードE2では、暗号化されたパケットを復号化する場合に、S P I=100のパケットとS P I=200のパケットは、異なる暗号処理装置S Pで復号化を行う。このとき、両方の暗号処理装置は、同じ暗号化アルゴリズムおよび鍵を使用する。

【0105】なお、セキュリティパラメータインデックス(S P I)と暗号処理装置(S P)との対応情報は、

セキュリティデータベース（SD）内に保持してもよいし、セキュリティデータベース（SD）外に保持してもよい。

【0106】ところで、ハッシュキーとしては、あるセレクタにマッチするパケットの中で複数のハッシュ値Hが計算され得るようなもので、Hの値が異なるパケット間では順序保証の必要がないようなものを選択する。図5にこの条件を満たすようなセレクタとハッシュキーの組合せの一例を示す。なお、本実施形態では、図5の5番目のエントリのハッシュキーを使用して、ハッシュキーとして送信元アドレスを使用している。

【0107】図5の最初のエントリは、セレクタは宛先アドレスまたは宛先アドレスのリスト（あるいは連続した値であるときには宛先アドレスのレンジでもよい）であり、このとき、ハッシュキーとして、送信元アドレスが使用される。

【0108】2番目のエントリは、セレクタは送信元アドレスまたは送信元アドレスのリスト（あるいは連続した値であるときには送信元アドレスのレンジでもよい）であり、このとき、ハッシュキーとして、宛先アドレスが使用される。

【0109】3番目のエントリは、セレクタは送信元アドレスと宛先アドレスの組であり、このとき、ハッシュキーとして、送信元ポート番号と宛先ポート番号の組が使用される。

【0110】4番目のエントリは、セレクタは送信元ポート番号と宛先ポート番号の組であり、このとき、ハッシュキーとして、送信元アドレスと宛先アドレスの組が使用される。

【0111】5番目のエントリは、セレクタはトンネルの出口アドレスであり、このとき、ハッシュキーとして、上記ハッシュキーの任意の組合せが使用される。

【0112】あるハッシュキーからハッシュ値Hを計算する方法は、例えば、

$$H = K \bmod N$$

とする。ここで、Kは、与えられたハッシュキーを1バイトごとのブロックに区切り、各ブロックを加算することにより得られた1バイトの符号なし整数値であり、Nは、ハッシュ値の最大値である。

【0113】次に、本暗号通信システムの第3の構成例について説明する。

【0114】ここでは、IPsecにおいて、（同一のトンネル出口ノードアドレスに対して、）セキュリティパラメータインデックス（SPI）は互いに異なるが、セキュリティプロトコルと暗号化アルゴリズムと鍵情報は全て同一であるような複数のセキュリティアソシエーションの設定を許容し、それらセキュリティアソシエーション間で暗号化処理の並列化を行う場合において、パケット内に記述されて転送されるSPIにハッシュ値を埋め込む場合について説明する。

【0115】まず、図6に、セキュリティパラメータインデックスSPIのフォーマットを示す。

【0116】セキュリティパラメータインデックスSPIは、「SA識別用フィールド」と、「ハッシュフィールド」とに分割される。両フィールドの境界は可変であるが、暗号化側のノードと復号化側のノードで同じ設定にするなどして、境界が分かるようにする。

【0117】次に、このセキュリティパラメータインデックス（SPI）を用いた暗号処理を行うIPsecネットワークの例を示す。

【0118】ネットワーク構成は図1の例と同様である。

【0119】図7に、ノードE1やノードE2が管理するセキュリティデータベース（SD）の一例を示す。

【0120】図7では、まず、トンネル出口のノードのアドレスがE2であるようなパケットは、すべて暗号化されてトンネル上で転送され、トンネル出口のノードのアドレスがE2以外であるようなパケットは廃棄される。

20 20 【0121】また、トンネルの出口がノードE2であるようなパケットは、セキュリティプロトコル=ESP、暗号化アルゴリズム=A1、鍵=K1を持ち、SPIが異なる、複数のセキュリティアソシエーション（SA）のいずれかにマッピングされる。

【0122】ここで、一例として、ハッシュフィールド長N=2ビットとし、SPIのSA識別用フィールド値=1000とすると、i=0、1、2、3の4種類のハッシュ値が使用可能であり、その結果、4種類のSPI=1000×(2^N) + i = 1000×4 + i (0 ≤ i < 4)のいずれかにマッピングされる。

30 30 【0123】4種類のSPI=1000×4 + i (0 ≤ i < 4)のいずれかにマッピングされるパケットの暗号化前のIPパケットヘッダおよびまたはIPペイロードのフィールドの全部または一部の情報から、第2の構成例のところで説明したものと同様にして計算されたハッシュ値をHとすると、このパケットには、SPI=400+Hがマッピングされる。

【0124】このとき、ノードE1において2台の暗号処理装置を使用するものとすると、例えば、図8に示すように、SPI=4のパケットとSPI=5のパケットを#1の暗号処理装置SPで暗号化処理し、SPI=6のパケットとSPI=7のパケットを#2の暗号処理装置SPで暗号化処理する。同様に、ノードE1において2台の暗号処理装置を使用するものとすると、SPI=4のパケットとSPI=5のパケットを#1の暗号処理装置SPで復号化処理し、SPI=6のパケットとSPI=7のパケットを#2の暗号処理装置SPで復号化処理する。

50 50 【0125】次に、本暗号通信システムの第4の構成例について説明する。

【0126】ここでは、IPsecのトンネルモードにおいて、SPI以外のフィールドにハッシュ値を埋め込む場合について説明する。

【0127】IPv4の場合には、「インターネットRFC791」にて規定されるIPv4ヘッダの「Type of Serviceフィールド」にハッシュ値を入れる。

【0128】IPv6の場合には、「インターネットRFC2460」にて規定されるIPv6ヘッダの「Traffic Classフィールド」または「Flow Labelフィールド」にハッシュ値を入れる。

【0129】また、IPsecトンネルがMPLS (Multi-Protocol Label Switching) のラベルスイッチングバスで実現される場合には、「インターネットドラフトdraft-ietf-mpls-label-encaps-03.txt」にて指定されるMPLSラベルヘッダの「Experimental Use」ビットにハッシュ値を入れる。

【0130】このとき、図9に示されるように、第2の構成例のところで説明したものと同様にしてハッシュ値Hが計算され、該ハッシュ値Hが上記フィールドに埋め込まれ、ノードE1, E2では、H=0または1のパケットとH=2または3のパケットとを異なる暗号処理装置で処理する。

【0131】なお、ここではハッシュ値のみで処理する暗号処理装置(SPI)を決定するが、ハッシュ値とSPI値の両方を用いて処理する暗号処理装置(SPI)を決定してもよい。

【0132】次に、SPIの値から各暗号処理装置(SPI)への暗号処理の振り分け方法について説明する。

【0133】図10に、SPIにハッシュ値を埋め込まない場合の振り分け方法の一例を、図11にSPIにハッシュ値を埋め込む場合の振り分け方法の一例を、図12にSPI以外のフィールドにハッシュ値を埋め込む場合の振り分け方法の一例をそれぞれ示す。

【0134】暗号側と復号側の各ノードにおいて、並列化する各暗号処理装置(SPI)には、番号がついているものとする。

【0135】図10において、 $SPI = a$ のパケットは番号1の暗号処理装置で、 $SPI = b_1, b_2$ のパケットは番号2の暗号処理装置で、 $SPI = b_3$ のパケットは番号3の暗号処理装置で処理される。

【0136】図11において、SA識別フィールド=aのパケットは、番号($H \bmod M_1$)の暗号処理装置で処理され、SA識別フィールド=bのパケットは、番号($M_1 + (H \bmod M_2)$)の暗号処理装置で処理される。ここで、M1, M2は、それぞれ、SA識別フィールド=a, bのパケットが使用可能な暗号処理装置の数を表し、ハッシュ値HはSPIのハッシュフ

ィールドの値を表す。

【0137】図12においては、SPIのハッシュフィールドのみで暗号処理装置の振り分けが行われる。すなわち、ハッシュフィールドHのパケットは、番号($H \bmod M$)の暗号処理装置で処理される。ここで、Mは、暗号処理ノードが使用可能な暗号処理装置の数を表す。

【0138】図10と図11のいずれの方法を用いても、例えば、アルゴリズムが異なるセキュリティアソシエーション間では暗号処理装置を共有せず、アルゴリズムが同じ各セキュリティアソシエーションの中で暗号処理装置を共有するような制御が可能である。また、図12の方法を用いると、すべてのセキュリティアソシエーションの間で暗号処理装置を共有することが可能になる。

【0139】次に、暗号化側パケット処理、復号化側パケット処理の手順について説明する。

【0140】図13に、本発明による暗号化側パケット処理のフローチャートを示す。また、図14に、本発明による復号化側パケット処理のフローチャートを示す。

【0141】なお、図13および図14において、セキュリティプロトコルが認証ヘッダの場合には、「暗号化」='認証情報付与'、「復号化」='認証'と置き換えて本フローチャートを適用する。また、セキュリティプロトコルが認証情報つきの暗号化ペイロードである場合には、「暗号化」='暗号化および認証情報付与'、「復号化」='認証および復号化'と置き換えて同じフローチャートを適用する。

【0142】まず、図13を参照しながら、暗号化側パケット処理の手順について説明する。

【0143】Pを暗号化前のパケット、E1をパケットPの暗号化側のノード(トンネルの入口ノード)のアドレス、E2をパケットPの復号化側のノードのアドレスとする(ステップS11, S12)。

【0144】まず、ステップS13で、セキュリティデータベースSDを検索し、パケットPにベストマッチするセレクタを探し、これをSとする(マッチするセレクタが見つからなければ、Sとして空の値(NULL)が返される)。次に、セレクタSに関するセキュリティポリシーをPoとする(SがNULLなら、Po="廃棄"となるものとする)。

【0145】セキュリティポリシーPoが"廃棄"であれば(ステップS14)、パケットPを廃棄して(ステップS15)、処理を終了する。

【0146】セキュリティポリシーPoが"非暗号化"であれば(ステップS14)、パケットP':=パケットPとし(ステップS16)、パケットP'を、宛先アドレス=E2、送信元アドレス=E1のIPパケットにカプセル化して送信する(ステップS22)。

【0147】セキュリティポリシーPoが"暗号化"で

あれば（ステップS14）、 P_r をセレクタSに対するセキュリティプロトコルとし、またA=（セレクタS、アドレスE2、セキュリティプロトコル P_r ）とし（ステップS17）、パケットPにセレクタS用のハッシュ関数を適用したときのハッシュ値Hを計算する（ステップS18）。次に、Aが使用可能なセキュリティパラメータインデックスS P Iのうち、ハッシュ値Hに対応する値Iを選択する（ステップS19）。

【0148】最後に、MをS P I値Iに対して使用される暗号処理装置S Pの番号として（ステップS20）、番号Mの暗号処理装置S Pにおいて、パケットPを、Aが使用する暗号化アルゴリズムおよび鍵を用いて暗号化し（ステップS21）、暗号化後のパケットP'を、宛先アドレス=E2、送信元アドレス=E1のIPパケットにカプセル化して送信する（ステップS22）。

【0149】次に、図14を参照しながら、復号化側パケット処理の手順について説明する。

【0150】PをIPカプセル化されたペイロード、E2をパケットPに対する復号化側ノード（トンネル出口ノード）のアドレス、 P_r をパケットPのヘッダ中のプロトコル番号から決定されるセキュリティプロトコルとする（ステップS31）。

【0151】セキュリティプロトコル P_r がAH（認証ヘッダ）またはESP（暗号化ペイロード）のいずれでもなければ（ステップS32）、パケットP':=パケットPとし、またSをパケットP'にベストマッチするセレクタ、 P_o をセレクタSに対するポリシーとし（ステップS33、S34）、ポリシー P_o が“非暗号化”でなければ、パケットP'を廃棄し（ステップS35、S37）、ポリシー P_o が“非暗号化”であれば、パケットP'を次段ルータに送信する（ステップS35、S38）。

【0152】一方、ステップS32で、セキュリティプロトコル P_r がAH（認証ヘッダ）またはESP（暗号化ペイロード）のいずれかであれば、パケットPはセキュリティパラメータインデックスS P Iの情報を含むので、IをパケットPに対するS P Iとし、またA=（S P I値I、アドレスE2、セキュリティプロトコル P_r ）、MをS P I値Iに対して適用される暗号処理装置S Pの番号として（ステップS39）、番号Mの暗号処理装置S Pにおいて、パケットPを、セキュリティアソシエーションAが使用する復号化アルゴリズムおよび鍵を用いて復号化し、復号化後のパケットP'とする（ステップS40）。

【0153】復号化に成功した場合には（ステップS41）、次に、S P I値Iに対するセレクタをS、パケットP'にベストマッチするセレクタをS'、セレクタSに対するポリシーを P_o とし（ステップS42）、S=S'かつ P_o =“暗号化”であれば、パケットP'を次段ルータに送信し（ステップS36、S38）、そうで

なければ（セキュリティポリシーに反するパケットであるとみなされるため）、パケットP'を廃棄する（ステップS36、S37）。

【0154】もしステップS40での復号化に失敗した場合には（ステップS41）、パケットP'を廃棄して（ステップS37）、処理を終了する。

【0155】なお、図13および図14において、S A識別情報=（トンネル出口アドレス、S P I、セキュリティプロトコル）を見て異なる暗号処理装置S Pにパケットを振り分ける場合には、「M:=Iが使用する暗号処理装置S Pの番号」の部分が「M:=Aが使用する暗号処理装置S Pの番号」に置き換えられる。

【0156】次に、暗号処理ノードの構成について説明する。

【0157】図15に、図13（暗号側）および図14（復号側）の両方動作を実現するノードの構成例を示す。

【0158】本暗号処理ノードは、パケット入力部21、ヘッダ解析部22、自ノード宛パケット処理部23、セキュリティプロセッサ振分け部（S P振分け部）24、セキュリティデータベース（SD）25、復号化セキュリティプロセッサ（以下、復号化S P）26、復号化側セキュリティポリシー決定部27、フォワーディング処理部28、パケット出力部29、暗号化側セキュリティポリシー決定部30、ハッシュ計算部31、暗号化セキュリティプロセッサ（以下、暗号化S P）32、カプセル化ヘッダ付加部33を備えている。

【0159】なお、暗号化S Pと復号化S Pとを組にして設ける場合には、その1組がこれまでの1つの暗号処理装置に相当する。暗号化S Pと復号化S Pとを独立に設ける場合には、個々の暗号化S Pや復号化S Pがこれまでの暗号処理装置に相当する（ここでは、前者とする）。

【0160】本暗号処理ノードは、パケット入力部21からパケットを受信すると、ヘッダ解析部22にて宛先アドレスのチェックを行う。

【0161】まず、宛先アドレスが自ノードアドレスである場合について説明する。

【0162】この場合、プロトコルIDフィールドが、セキュリティプロトコルまたはIPカプセル化を表すものでなければ、自ノード宛パケット処理部23にてプロトコルIDフィールドにて示される上位レイヤプロトコル処理を行う。

【0163】一方、プロトコルIDフィールドがセキュリティプロトコルを示すものであれば、S P振分け部24にパケットを渡す。

【0164】パケットを受けたS P振分け部24では、セキュリティデータベース（SD）25を検索し、受信パケットのペイロード部に書かれているセキュリティパラメータインデックス（S P I）にマッチするエントリ

があれば、そのエントリに対して使用される暗号化アルゴリズム、鍵情報を用いて、S P Iから一意に決定される復号化S P 2 6にてペイロードの復号化処理を行う。

【0165】次に、復号化側セキュリティポリシー決定部2 7において、上記復号化処理により得られるパケットのヘッダとセキュリティデータベース(S D)2 5の内容とから、パケットをフォワード可能かどうかを決定する。可能であれば、フォワーディング処理部2 8にて出力インターフェースを決め、パケット出力部2 9からパケットを出力する。

【0166】続いて、宛先アドレスが自ノードアドレスでない場合について説明する。

【0167】この場合、まず、暗号化側セキュリティポリシー決定部3 0にて、セキュリティデータベース(S D)2 5の検索を行う。

【0168】もし、受信パケットのヘッダ情報にマッチするようなセキュリティデータベースのエントリ(S Dエントリ)がなければ、パケットを廃棄する。

【0169】一方、そのようなS Dエントリがある場合には、もし、パケットを暗号化する必要がなく且つカプセル化する必要がなければ、フォワーディング処理部2 8にて出力インターフェースを決め、パケット出力部2 9からパケットを出力する。

【0170】また、もし、パケットを暗号化する必要がなく且つカプセル化する必要があれば、カプセル化ヘッダ付加部3 3にてカプセル化ヘッダを付加した後、フォワーディング処理部2 8にて出力インターフェースを決め、パケット出力部2 9からパケットを出力する。

【0171】もし、パケットを暗号化する必要があれば、受信パケットのヘッダ情報とともにハッシュ計算部3 1にてハッシュを計算し、ハッシュ値から一意に決まる暗号化S P 3 2において、受信パケットにマッチしたS Dエントリにて指定される暗号化アルゴリズム鍵を用いて、パケットの暗号化を行う。その後、カプセル化ヘッダ付加部3 3にてカプセル化ヘッダを付加した後、フォワーディング処理部2 8にて出力インターフェースを決め、パケット出力部2 9からパケットを出力する。

【0172】なお、上記では、図1 3(暗号側)および図1 4(復号側)の両方動作を実現するノードの構成例を示したが、図1 3(暗号側)または図1 4(復号側)のいずれか一方のみを実現するノードを構成することも可能である。

【0173】次に、暗号処理ノードのハード構成について説明する。

【0174】図1 6に、本暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノード内に配置した場合のハード構成の一例を示す。

【0175】図1 6において、暗号処理ノードは、スイッチ部4 1、ネットワークインターフェース部4 2、内部処理インターフェース部4 3、および(C P U 4 4 1

+メモリ4 4 2を含む)中央処理部4 4を備える。

【0176】なお、スイッチ部4 1を用いるかわりに、内部バスを用いることにより、スイッチ部4 1、ネットワークインターフェース部4 2、内部処理インターフェース部4 3、および中央処理部4 4間のデータ転送を実現してもよい。

【0177】各ネットワークインターフェース部4 2は、セキュリティデータベースS DおよびフォワーディングテーブルF Wを持つ。また、各内部処理インターフェース部4 3は、セキュリティプロセッサ部(暗号処理装置に相当)S PおよびフォワーディングテーブルF Wを持つ。中央処理部4 4は、自ノード宛のI PパケットのうちペイロードがI PのP D Uでないもの(I P-i n-I Pでないもの)に対する処理および、フォワーディングテーブルF W、セキュリティデータベースS D、セキュリティプロセッサ部S Pの管理を行う。

【0178】本暗号処理ノードは、パケットをネットワークインターフェース部4 2から受信した場合には、まず、パケットの宛先アドレスが自ノードのアドレスと一致するかどうかを調べ、一致しない場合には、以下の処理を行う。

【0179】まず、ネットワークインターフェース部4 2内のフォワーディングテーブルF Wを参照してトンネル出口のアドレスを決定する。次に、セキュリティデータベースS Dを参照し、セキュリティパラメータインデックスS P I、および処理すべき内部処理インターフェース部4 3を決定した後、受信パケット、トンネル出口のアドレス、S A識別情報、およびS P Iを、スイッチ部4 1を通して、決定した内部処理インターフェース部4 3に送信する。

【0180】内部処理インターフェース部4 3では、トンネル出口のアドレスをキーに内部処理インターフェース部4 3内のフォワーディングテーブルF Wを参照して、指定されたトンネル出口アドレスに対する出力ネットワークインターフェース部4 2を決定する。次に、必要であれば受信パケットをセキュリティプロセッサ部S Pで暗号化処理した後、宛先アドレス=トンネル出口アドレス、送信元アドレス=出力ネットワークインターフェース部4 2のネットワークアドレスとしたパケットヘッダを付加し、スイッチ部4 4 1を通して、出力ネットワークインターフェース部4 2に送信する。

【0181】出力ネットワークインターフェース部4 2は、スイッチ部4 1から出力されたパケットに対して、レイヤ2処理を行った後、これを外部に出力する。

【0182】一方、ノードがパケットをネットワークインターフェース部4 2から受信した場合に、パケットの宛先アドレスが自ノードのアドレスと一致する場合には、以下の処理を行う。

【0183】まず、ペイロードがI PのP D Uでない場合には、パケットを中央処理部4 4に送信する。そうで

なければ、セキュリティデータベースSDを参照し、SA識別情報および処理すべき内部処理インターフェース部43を決定した後、受信パケットのペイロード、SPI(受信パケットがSPIを持たなければNULL値となる)を、スイッチ部41を通して、決定した内部処理インターフェース部43に送信する。

【0184】内部処理インターフェース部43では、必要であればペイロードをセキュリティプロセッサ部SPで復号化処理した後、復号化後のペイロード(=暗号化前のPDU)の先頭部に存在する暗号化前のパケットヘッダの宛先アドレスをキーに、内部処理インターフェース部43内のフォワーディングテーブルFWを参照して、指定された宛先アドレスに対する出力ネットワークインターフェース部42を決定し、スイッチ部41を通して、出力ネットワークインターフェース部42に送信する。

【0185】出力ネットワークインターフェース部42は、スイッチ部41から出力された復号化後のペイロード(=暗号化前のPDU)、レイヤ2処理を行った後、これを外部に出力する。

【0186】次に、図17に、本暗号処理ノードの構成として、並列処理を行うセキュリティプロセッサをノード内に配置した場合のハード構成のもう一つの例を示す。

【0187】図17において、暗号処理ノードは、スイッチ部61、ネットワークインターフェース部62、セキュリティプロセッサ部(暗号処理装置に相当)63、中央処理部64を備えている。また、中央処理部64は、CPU6411とメモリ6412を含むユニット641と、1組または複数組のセキュリティデータベースSDおよびフォワーディングテーブルFW6421を含むユニット642を持つ。

【0188】なお、スイッチ部61を用いるかわりに、内部バスを用いることにより、スイッチ部61、ネットワークインターフェース部62、内部処理インターフェース部63、および中央処理部64間のデータ転送を実現してもよい。

【0189】中央処理部64は、自ノード宛のIPパケットのうちペイロードがIPのPDUでないもの(IP-in-IPでないもの)に対する処理、および、フォワーディングテーブルFW、セキュリティデータベースSD、セキュリティプロセッサ部SPの管理を行う。

【0190】暗号処理ノードは、パケットをネットワークインターフェース部62から受信した場合には、まず、スイッチ部61を通して中央処理部64に受信パケットを転送する。

【0191】中央処理部64では、まず、パケットの宛先アドレスが自ノードのアドレスと一致するかどうかを調べ、一致しない場合には、フォワーディングテーブルFWを参照してトンネル出口のアドレスを決定する。次

に、セキュリティデータベースSDを参照し、セキュリティパラメータインデックスSPI、および処理すべきセキュリティプロセッサ部SPを決定した後、受信パケット、およびSPIを、スイッチ部61を通して、決定したセキュリティプロセッサ部SPに送信する。

【0192】セキュリティプロセッサ部SPでは、必要であれば受信パケットを暗号化処理した後、SPIとともにスイッチ部61を通して中央処理部64に送信する。

【0193】中央処理部64は、SPIからトンネルの出口ノードのアドレスを求め、宛先アドレス=トンネル出口アドレス、送信元アドレス=出力ネットワークインターフェース部62のネットワークアドレスとしたパケットヘッダを付加し、スイッチ部61を通して、出力ネットワークインターフェース部62に送信する。

【0194】出力ネットワークインターフェース部62は、スイッチ部61から出力されたパケットに対して、レイヤ2処理を行った後、これを外部に出力する。

【0195】一方、中央処理部64において、パケットの宛先アドレスが自ノードのアドレスと一致する場合には、ペイロードがIPのPDUでない場合にはパケットをCPUに渡す。そうでなければ、セキュリティデータベースSDを参照し、セキュリティパラメータインデックスSPI、および処理すべきセキュリティプロセッサ部SPとを決定した後、受信パケットのペイロード、SPI(受信パケットがSPIを持たなければNULL値となる)を、スイッチ部61を通して、決定したセキュリティプロセッサ部SPに送信する。

【0196】セキュリティプロセッサ部SPでは、ペイロードを、必要であれば復号化処理後、スイッチ部を通して、中央処理部64に送信する。

【0197】中央処理部64は、スイッチ部61から出力されたペイロードをパケットのPDUとみなし、そのパケットのヘッダの宛先アドレスをキーにフォワーディングテーブルFWを参照して、指定された宛先アドレスに対する出力ネットワークインターフェース部62を決定し、スイッチ部61を通して、出力ネットワークインターフェース部62に送信する。

【0198】出力ネットワークインターフェース部62は、スイッチ部61から出力されたパケットに対してレイヤ2処理を行った後、これを外部に出力する。

【0199】次に、本実施形態のようなセキュリティパラメータインデックス(SPI)の使用方法を可能にするセキュリティアソシエーション(SA)の確立方法について説明する。

【0200】図18に、この場合のセキュリティアソシエーションの確立手順の一例を示す。

【0201】図18において、暗号化側ノードE1と復号化側ノードE2は、SPI=100, 200に対し、同じセキュリティプロトコル“ESP”、同じ暗号

化アルゴリズム“3DES”、同じ鍵情報“X”を持つように、2つのデータ転送用のセキュリティアソシエーション(SA)を確立することを目的とする。このとき、SPI=100のパケットと、SPI=200のパケットは、並列処理が可能である。

【0202】まず、ノードE1は、上記データ転送用のセキュリティアソシエーションをセキュア且つ自動的に確立するために使われるISAKMPセッション用のセキュリティアソシエーションを確立する。

【0203】暗号化側ノードは、まず、上記データ転送用セキュリティアソシエーションを確立するためのISAKMP用のセキュリティアソシエーションを確立するために、(Hdr, SA-NP(proto, algo, SPI); KE; ID)を持つISAKMPパケットを送信する。ここで、HdrはISAKMPパケットヘッダ、SA-NPは1個以上のプロポザル・ペイロードとトランスフォーム・ペイロードを持つSAネゴシエーション・ペイロード、protoはセキュリティプロトコル、algoは暗号化アルゴリズム、KEは鍵情報、IDはセレクタの識別情報を表す。

【0204】ノードE2は、これに対する応答として、(Hdr, SA-NP(proto, algo, SPI); KE; ID; AUTH)を返す。

【0205】ここで、AUTHはノードE2に対する認証情報である。

【0206】次に、ノードE1は、これに対する応答として、(Hdr*, AUTH*)を返す。ここで、AUTHはノードE2に対する認証情報である。また、“*”つきのフィールドは暗号化されていることを示す。

【0207】上記手続きによりISAKMPセッション用のセキュリティアソシエーションを確立すると、データ転送用のセキュリティアソシエーションを同様の手続きにより行う。ここで、既にISAKMP用のセキュリティアソシエーションが確立しているため、データ転送用のセキュリティアソシエーションに使用されるパケットのすべてのフィールドは暗号化されている。

【0208】なお、本実施形態では、セキュリティアソシエーション確立時に、ISAKMPパケットにセキュリティプロセッサ部の数に関する情報(並列度)を含めてもよい。これは、上記並列度を、ISAKMPのVendor IDペイロードに含めることにより可能となる。この情報は、ハッシュ関数を計算する際に利用される。例えば、暗号化側ノードの並列度がMで、復号化側ノードの並列度がNの場合には、ハッシュ値の個数をL=LCM(M, N)の最小公倍数に設定すれば、パケットが取るハッシュ値が平均的に均一になるようにパケットが到着していれば、どの暗号化ノード、復号化側ノードの両方で、均一に複数の暗号処理プロセッサ部に暗号処理を分散させることができる。

【0209】また、本実施形態では、セキュリティアソ

シエーション確立時に、セキュリティパラメータインデックスSPIをSA識別用のフィールドと、ハッシュ値用のフィールドの2つのサブフィールドに分割する場合に、2つのサブフィールドの境界に関する情報(例えば、SA識別情報の長さ)をISAKMPパケットに含めてもよい。これは、上記フィールド境界に関する情報情報を、ISAKMPのVendor IDペイロードに含めることにより可能となる。

【0210】次に、本発明で使用される暗号化パケットのフォーマットについて説明する。

【0211】図19に、本発明で使用される暗号化パケットのフォーマットを示す。(a)がセキュリティプロトコルがAHの場合であり、(b)がESPの場合である。

【0212】(a), (b)において、オリジナルのIPヘッダおよびオリジナルのIPペイロードの部分が、暗号化される前および復号化された後のIPパケットに対応し、それ以外の部分が、暗号化パケットで新たに附加された部分である。また、(a)においては、オリジナルのIPヘッダおよびオリジナルのIPペイロードの部分が暗号化され、(b)においては、それらに加えてパディング等の部分も暗号化される。

【0213】なお、セキュリティプロトコルは、新IPヘッダ(IPカプセル化する際に付与されるヘッダ)の中のプロトコル番号で指定される。IPv4、IPv6ともに図19のようなフォーマットを使用する。ただし、IPv6の場合には、ESPは拡張ヘッダとして扱われるのに対し、IPv4の場合には、ペイロードとして扱われる。

【0214】また、AH、ESPとともに、シーケンス番号のためのフィールドを持つ。これは、SA識別情報が異なればシーケンス番号空間が異なることを表す。したがって、本発明において、同じセキュリティプロトコル、暗号化アルゴリズム、鍵情報に対して、複数のSA識別情報を割り当てる場合には、これらのSA識別情報は異なるシーケンス番号空間を持つ。

【0215】なお、本実施形態で使用するハッシュ値は、様々な算術演算、ビット単位の操作、テーブルによる変換、それらを組み合わせたもの等による変換により求めた値で代用することもできる。この変換は、入力値に対して確定的に演算値が定まり、入力値の種類よりも少ない(もしくは非常に少ない)種類の複数の演算値を取るものであって、複数種類の入力値がなるべく均等に分散して複数種類の演算値に振り分けられるようなものがほしい。

【0216】また、ルータと暗号処理ノードとは一体となっていてもよく、またルータと暗号処理ノードが独立であってもよい。ルータと暗号処理ノードとが独立の場合には、それらはネットワークを介して接続してもよく、さらに複数のルータで1つ以上の暗号処理ノードを

共有してもよい。

【0217】また、本発明は、IPsecだけでなく、SA識別情報をパケットに付加するような任意のレイヤのセキュリティプロトコルに対して適用可能である。

【0218】また、本発明は、暗号側と復号側で異なる鍵情報を用いる方式にも適用可能である。この場合は、セキュリティパラメータインデックス(SPI)等に暗号側で使用する鍵情報と復号側で使用する鍵情報を対応付ければよい。

【0219】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0220】また、本実施形態は、コンピュータに所定の手段を実行させるための(あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための)プログラムを記録したコンピュータ読み取り可能な記録媒体としても実施することもできる。

【0221】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0222】

【発明の効果】本発明によれば、送信側ノード装置では、同一の暗号化アルゴリズムおよび鍵情報を適用して暗号処理を行うべき複数種類のパケットに、その種類毎に異なる識別子を付与し、受信側ノード装置では、受信したパケットに付与された識別子に基づいて複数の暗号処理装置のうちの一つを選択するようにしたので、順序保証を必要とするパケットについてその順序保証を可能にするとともに、処理の並列性を高めることができる。

【図面の簡単な説明】

【図1】本発明を適用する通信ネットワークの一例を示す図

【図2】本発明の一実施形態に係るセキュリティデータベースの構成例を示す図

【図3】同実施形態に係る動作の一例を説明するための図

【図4】同実施形態に係るセキュリティデータベースの他の構成例を示す図

【図5】同実施形態に係るセレクタとハッシュキーとの対応について説明するための図

【図6】同実施形態に係るセキュリティパラメータインデックスのフォーマット例を示す図

【図7】同実施形態に係るセキュリティデータベースのさらに他の構成例を示す図

【図8】同実施形態に係る動作の他の例を説明するための図

【図9】同実施形態に係る動作のさらに他の例を説明するための図

【図10】同実施形態に係る暗号処理の振り分け方法の一例を説明するための図

【図11】同実施形態に係る暗号処理の振り分け方法の他の例を説明するための図

【図12】同実施形態に係る暗号処理の振り分け方法のさらに他の例を説明するための図

【図13】同実施形態に係る暗号化側パケット処理の手順の一例を示すフローチャート

【図14】同実施形態に係る復号化側パケット処理の手順の一例を示すフローチャート

【図15】同実施形態に係るノード装置の構成例を示す図

【図16】同実施形態に係るノード装置のハードウェア構成の一例を示す図

【図17】同実施形態に係るノード装置のハードウェア構成の他の例を示す図

【図18】同実施形態に係るセキュリティアソシエーションの確立手順の一例を示す図

【図19】同実施形態に係る暗号化パケットのフォーマット例を示す図

【図20】従来の暗号通信について説明するための図

【符号の説明】

1…暗号化側ノード

2…復号化側ノード

9～11…ホスト

5, 6…ネットワーク

7, 8…暗号処理装置

3, 4, 25…セキュリティデータベース

21…パケット入力部

30 22…ヘッダ解析部

23…自ノード宛パケット処理部

24…セキュリティプロセッサ振分け部

26…復号化セキュリティプロセッサ

27…復号化側セキュリティポリシー決定部

28…フォワーディング処理部

29…パケット出力部

30…暗号化側セキュリティポリシー決定部

31…ハッシュ計算部

32…暗号化セキュリティプロセッサ

40 33…カプセル化ヘッダ付加部

41, 61…スイッチ部

42, 62…ネットワークインターフェース部

43…内部処理インターフェース部

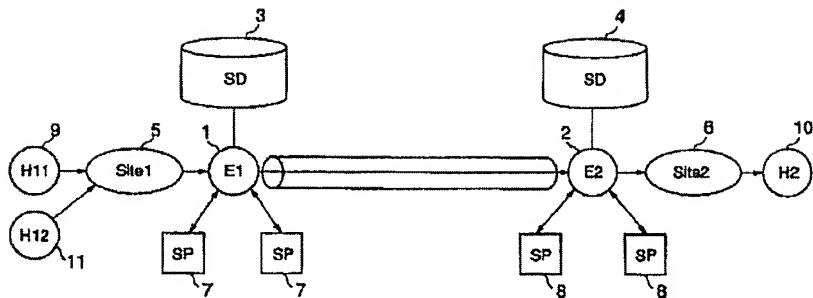
44, 64…中央処理部

63…セキュリティプロセッサ部

441, 6411…CPU

442, 6412…メモリ

【図1】



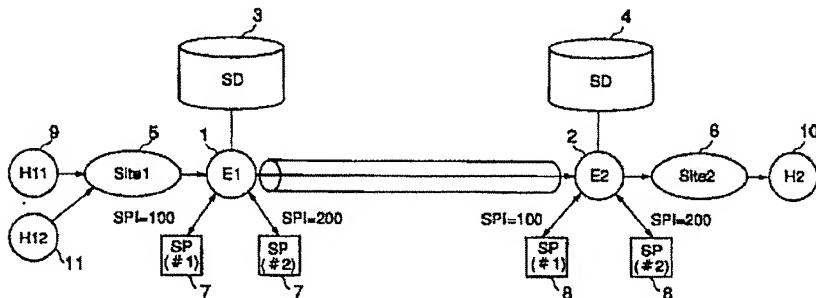
【図2】

トンネル出口	セレクタ	ポリシー	SPI	セキュリティプロトコル／アルゴリズム／鍵
E2	送信元アドレス=H11	暗号化	100	ESP/A1/K1
E2	送信元アドレス=H12	暗号化	200	ESP/A2/K2
E2	その他	非暗号化		
その他	指定なし	麻痺		

【図5】

セレクタ	ハッシュキー
対応アドレス(リスト)	送信元アドレス
送信元アドレス(リスト)	対応アドレス
送信元アドレス+対応アドレス	送信元ポート番号+対応ポート番号
送信元ポート番号+対応ポート番号	送信元アドレス+対応アドレス
トンネル出口アドレス	上記ハッシュキーの任意の組合せ

【図3】



【図4】

トンネル出口	セレクタ	ポリシー	H	SPI	セキュリティプロトコル／アルゴリズム／鍵
E2	指定なし	暗号化	0	100	ESP/A1/K1
E2	指定なし	暗号化	1	200	ESP/A1/K1
その他	指定なし	麻痺			

【図10】

SPI	SP番号
a	0
b1,b2	1
b3	2

【図6】

【図11】

SA識別用フィールド	ハッシュフィールド	SPI中のSA識別番号	SP番号
		a	H mod M1
		b	M1+(H mod M2)

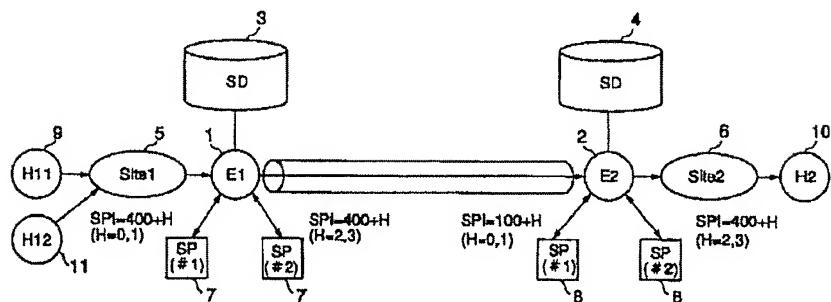
【図12】

SPI	SP番号
任意	H mod M

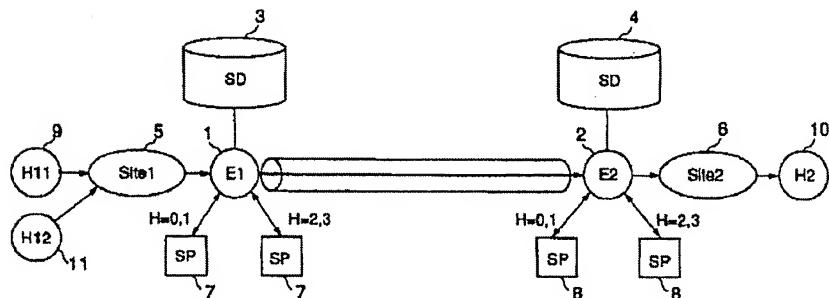
【図7】

トンネル出口アドレス	セレクタ	ポリシー	H	SPI	セキュリティプロトコル／アルゴリズム／鍵
E2	指定なし	暗号化	0..3	100*4+H	ESP/A1/K1
その他	指定なし	無効			

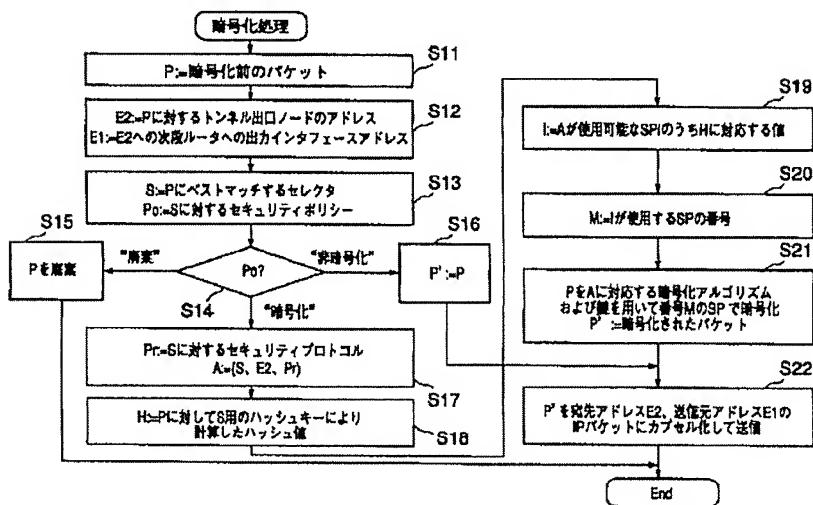
【図8】



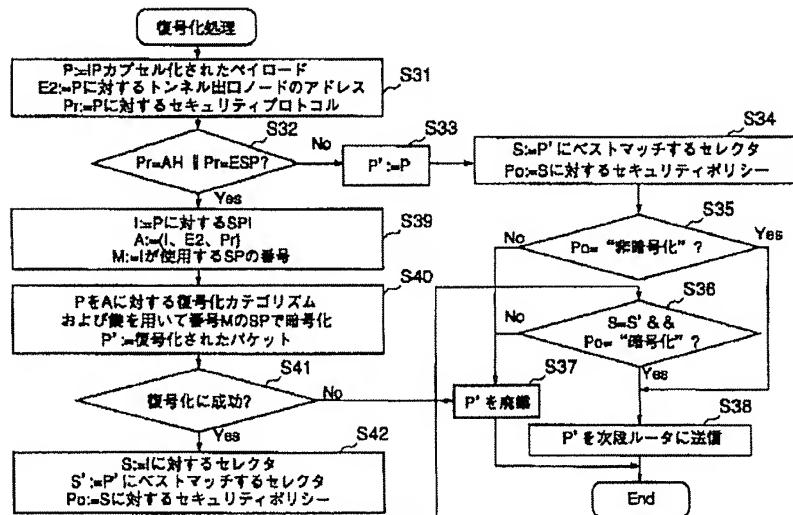
【図9】



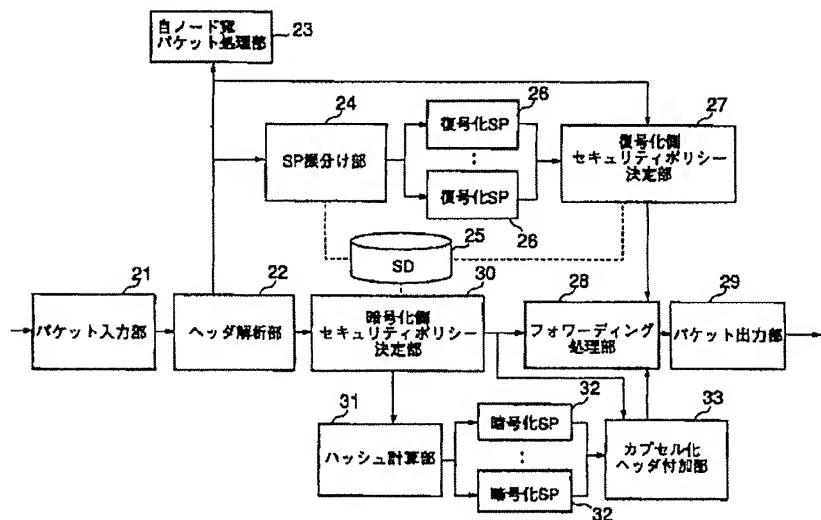
【図13】



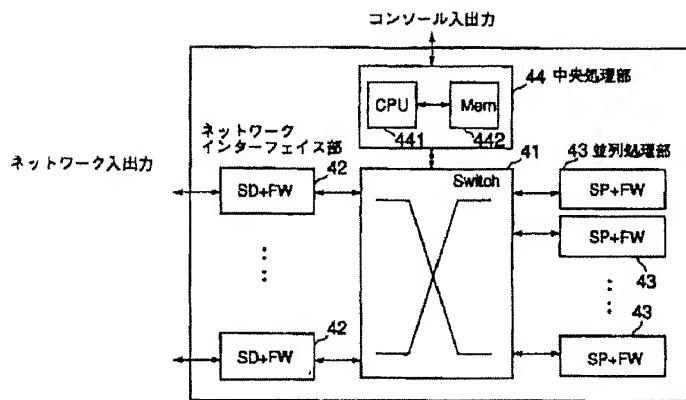
【図14】



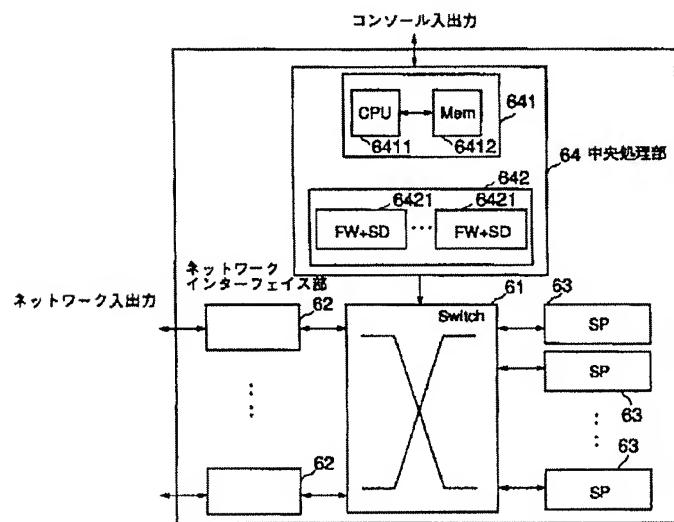
【図15】



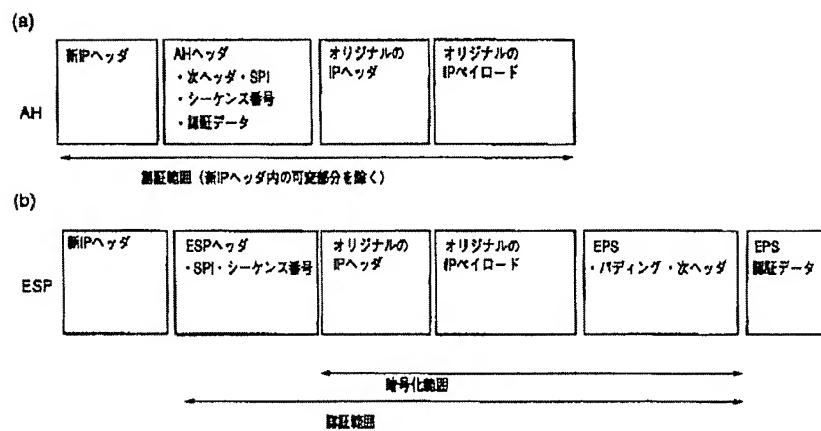
【図16】



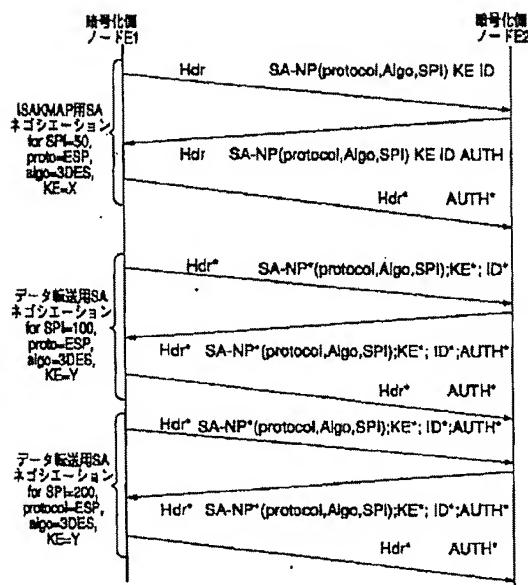
【図17】



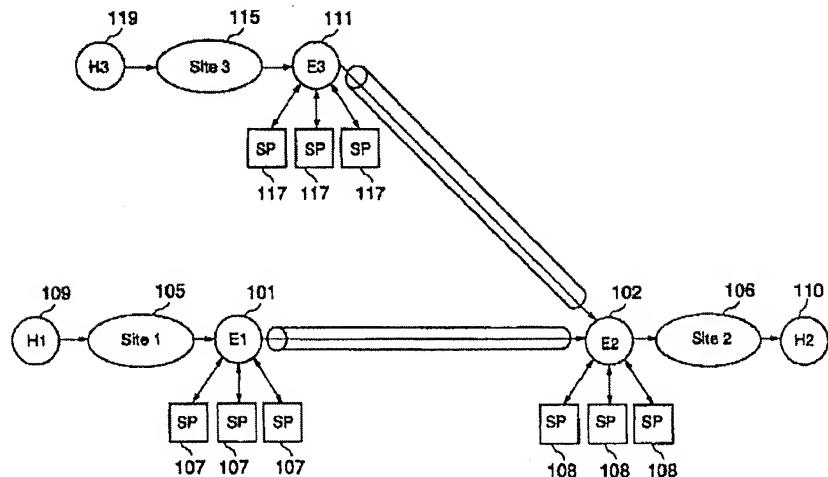
【図19】



【図18】



【図20】



フロントページの続き

Fターム(参考) 5J104 AA01 AA16 AA20 AA35 BA04
EA24 EA26 NA02 NA12 PA07
5K030 GA15 HB16 LA07 LB05 LD19
LE03 LE14
9A001 CC06 EE03 LL03